IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
(Attorney Docket № 15415US01)

In the Application of:

Sherman Chen, et al.

Electronically Filed on 06-APR-2010

Serial No. 10/769,173

Filed: January 30, 2004

For: A SECURE KEY AUTHENTICATION AND LADDER SYSTEM

Examiner: Yogesh Paliwal

Group Art Unit: 2435

Confirmation No. 7811

REPLY BRIEF

MS: APPEAL BRIEF-PATENTS
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with 37 CFR § 41.41, the Appellant submits this Reply Brief in response to the Examiner's Answer mailed on February 18, 2010. Claims 1-41 are pending in the present Application. The Appellant has responded to the Examiner in the Examiner's Answer, as found in the following Argument section.

As may be verified in his final Office Action (page 4), dated June 10, 2009 ("Final Office Action"), claims 1-41, all of which stand rejected under 35 U.S.C. § 103(a). *See* the Final Office Action at pages 5-6. To aid the Board in identifying corresponding

arguments, the Appellant has used the same headings in the Argument section of this Reply Brief as the headings found in the Appellant's corresponding Brief on Appeal. The Brief on Appeal has a date of deposit of November 18, 2009.

STATUS OF THE CLAIMS

Claims 1-41 were finally rejected. Pending claims 1-41 are the subject of this appeal.

ARGUMENT

I. The Proposed Combination of Akiyama and Ellison Does Not Render Claims 1-41 Unpatentable

A. Independent Claims 1, 11, 21 and 32

The Appellant stands by the argument made in the corresponding section of the Brief on Appeal.

In response to Appellant's Brief on Appeal, the Examiner is using the following argument stated on pages 10-12 of the Examiner's Answer:

> • Appellant argues (see pages 7-8 of appeal brief) that, "Referring to FIG. 5 of Akiyama, the Examiner has equated Applicant's "secure key" to Akiyama's "work key", which is part of Akiyama's contract information. Furthermore, Akiyama discloses that a separate master key is used to encrypt the work key, as illustrated in FIG. 3 and further explained in paragraph 0100 of Akiyama. However, the work keys of Akiyama are different from the master keys, which are used for encrypting the work keys. More specifically, Akiyama's master key is not a previously encrypted and signed work key (i.e., the master key is not generated by encrypting a previously generated signed work key). In this regard, Akiyama does not disclose that the work keys (equated by the Examiner to Applicant's "secure key") are encrypted utilizing a previously generated unreadable digitally signed and encrypted work key, where the previously generated unreadable digitally signed and encrypted work key was generated by encrypting a previously generated signed work key. In other words, Akiyama does not disclose that the work keys are encrypted using previously generated work keys, as recited in Applicant's claim 1. Ellison does not overcome the above deficiencies of Akiyama.
>
> • In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that **the features upon which applicant relies (i.e., "the work keys are encrypted using previously generated work keys") are not recited in the rejected claim(s)**. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See In re Van Geuns, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Examiner is interpreting the current language of the claim such that as long as the key that encrypt the secure key is also a secure key, it reads onto the claimed limitation. Since the master key of Akiyama is only provided to the subscriber through smart cards, the master key of Akiyama is in fact a **"secure key". Claim language does not require the key that encrypts the secure key to be of same type**. Furthermore appellant's own disclosure also allow the secure key to be any of master key,

> work key and/ or scrambling key (see claim 6 and paragraph 0028, "The secure key may be a master key, a work key and/or a scrambling key."). Therefore, appellant argument that if examiner interpret secure key to be work key then the key that encrypts the work key needs to be work key is not found persuasive. Therefore, the combination of Akiyama and Ellison still discloses all the limitations and the rejection should be maintained.

The Appellant respectfully disagrees, especially with the above bolded argument by the Examiner.

The Examiner, on numerous occasions in the Examiner's Answer and the Final Office Action, has alleged that the present specification does not disclose that if an encrypting module encrypts one type of secure key, then the encrypted output is the same type of secure key. In other words, the Examiner alleges that if, for example, a "master" key is encrypted, then the output is not a "master" key. The Appellant disagrees. First off, by virtue of the definition of the term "encrypting", the process of encrypting does not change the type of information being encrypted. Secondly, referring to Fig. 6 of the present application, the Appellant points out that module 604 is an encryptor (See present specification, at ¶49). In addition, the present specification clearly discloses that "master" decryption keys 620, 622 are input into the encryptor 604, and then the encryptor 604 generates secure (or encrypted) "master" decryption keys 624, 626 (*See id.*, at ¶49). In this regard, if an encrypting module encrypts one type of key, then the encrypted output is the same type of key, as evidenced by the functionality of the encryptor/scrambler 604. The Appellant further notes that similarly to module 604, module 608 is also an encryptor (*See id.*, at ¶52). Therefore, the signed "secure" key 638 (an input to the encryptor 608) is the same type (e.g., master key,

work key, or scrambling key) as the encrypted and signed "secure" key 632 (the output of the encryptor 608), based on at least the above arguments.

In response to the above bolded argument by the Examiner, the Appellant notes that the relevant language from Appellant's claim 1 is as follows:

> *encrypting the digitally signed secure key utilizing at least a previously generated unreadable digitally signed and encrypted secure key*, wherein said previously generated unreadable digitally signed and encrypted secure key was generated by encrypting a previously generated digitally signed secure key.

In other words, claim 1 recites that the secure keys are encrypted using previously generated secure keys. However, as explained above, if an encrypting module encrypts one type of key, then the encrypted output is the same type of key. In this regard, in instances when the secure key is a work key, then the statement that "work keys are encrypted using previously generated work keys" is a true and valid statement, supported by claim 1 and the specification, and contrary to what the Examiner alleges in the above bolded argument.

B. Examiner's Response to Arguments

In response to Appellant's Brief on Appeal, the Examiner is using the following argument stated on pages 12-14 of the Examiner's Answer:

> • Appellant further argues (see, pages 9-10 of appeal brief) that, "The Applicant submits that claim 1, as presented in the 08/11/08 response, indeed required that a secure key and a key that encrypts the secure key to be of same type. However, to further prosecution and to further clarify this aspect, the Applicant amended independent claims 1, 11, 21 and 32, as set forth in the 03/02/09 response and in the claim listing below. Support for the claim amendments may be found, for example, in Fig. 6A and paragraphs 46-54 of the specification. More specifically, referring to Applicant's Fig. 6A, the digitally signed secure keys 638 are encrypted by the encryptor 608. The encrypted and

signed secure keys 632 are looped back via the registers 610 and then communicated back (628 and 630) to the encryptor 608 for purposes of encrypting the next digitally signed secure key. Obviously, the digitally signed secure keys and the encrypted digitally signed secure keys are of the same type, the difference being that the latter have been encrypted and then looped back for purposes of using them during encryption of subsequent signed secure keys."

• **Examiner respectfully disagrees and still maintains that even Fig. 6A does not support applicant interpretation that requires secure key and key that encrypts the secure key to be of same type.** See paragraph 0047 (originally filed specification) that recites" In accordance with an aspect of the present invention, the master decryption keys 618 may be utilized in the encryption and decryption of one or more secure keys, for example, a work key and/or a scrambling key." Also note that claim 6 recites, "wherein if the secure key comprises a work key then a decrypted digitally signed master key at the second location is utilized for decrypting an encrypted digitally signed work key." This claim clearly establishes that when the secure key is a work key it has to be encrypted by the master key. Also see, claim 7 which recites, "wherein if the secure key comprises a scrambling key then a decrypted digitally signed work at the second location is utilized for decrypting an encrypted digitally signed scrambling key.". Examiner realizes that Fig. 6A in fact shows that after encrypting the secure key do go back to encrypt the next secure keys however, as recited at paragraph 0047 and claims 6 and 7, if the work key is looped back then it will encrypt the content key. Therefore, applicant's interpretation that secure key and key that encrypts the secure key to be of same type is not consistent with the specification and dependent claims 6 and 7. Nowhere in the specification it is recited that same level keys are encrypted using the same level keys as argued by the applicant. Also note that the current claim language does not raise rejection under U.S.C. 112 first paragraph for lacking the written description because at least one interpretation (one taken by the examiner) is supported by the specification. Examiner is interpreting the current language of the claim such that as long as the key that encrypt the secure key is also a secure key it reads onto the claimed limitation. Further note that even though applicant is interpreting secure key and key that encrypts the secure key to be of same type the current language of the claim is broad enough that as long as the key that encrypt the secure key is also secure it would read onto the claims limitation. **Further note that applicant's statement that "Obviously, the digitally signed secure keys and the encrypted digitally signed secure keys are of the same type, the difference being that the latter have been encrypted and then looped back for purposes of using them during encryption of subsequent signed secure keys" appears to be an opinion because there is no written description that requires these keys to be of same type.** As clearly shown by paragraph 0047 and claims 6 and 7, key that encrypts the digitally signed key is chosen based on what is the type of the digitally singed key is for example if the digitally signed key is work key then master key is used to encrypt the digitally signed key and if the digitally signed key is a scrambling

> key then work keys are used to encrypt the digitally signed key (see, paragraph 0041 and claims 6 and 7).

The Appellant respectfully disagrees, especially with the above bolded argument by the Examiner. Referring to Fig. 6A, the Appellant (see page 5 above) has explained that the signed and secure key 638 (input to encryptor 608) is of the same type as the encrypted and signed secure key 632 (output from encryptor 608). For example, in instances when the secure keys are work keys, then it is a true and valid statement that the signed work keys 638 are of the same type as the signed and encrypted work keys 632 (namely, both 638 and 632 are work keys). The same statement is valid if the secure keys are master keys (then both input and output of encryptor 608 are master keys), or if the secure keys are scrambling keys (then both the input and output of the encryptor 608 are scrambling keys). In addition, the signed and encrypted work keys 632 coming as output out of the encryptor 608, are the same as keys 628 and 630. (See present specification at, e.g., ¶¶52-53). In accordance with an exemplary aspect of the invention, these signed and encrypted work keys 628 and 630 can then be used by the encryptor 608 to encrypt subsequent secure keys. (*See id.*, e.g., at ¶53). The Applicant notes that ¶53 of the present specification allows, in one scenario, the encryptor 608 to use the master decryption keys 624, 626, and in another scenario, to use the signed and encrypted keys 628 and 630.

Therefore, the Appellant maintains that secure keys (e.g., 638) and keys (e.g., 628, 630) that encrypt the secure keys can be of the same type. In addition, the Appellant's statement that "Obviously, the digitally signed secure keys and the encrypted digitally signed secure keys are of the same type, the difference being that

the latter have been encrypted and then looped back for purposes of using them during encryption of subsequent signed secure keys" is a statement that is fully supported by the specification and figures.

In response to Appellant's Brief on Appeal, the Examiner is using the following argument stated on pages 16-17 of the Examiner's Answer:

> • Appellant further argues (on page 14) that, Again, the issue is not what level keys are used by the encryptor 608 to encrypt a digitally signed secure key 638, as represented by the Examiner. The issue is how the "previously generated unreadable digitally signed and encrypted secure key" (i.e., the digitally signed and encrypted secure key 632 coming as output out of the encryptor 608, being the same as key 628 or 630) is in fact generated. In other words, regardless of whether a master key is used to encrypt a secure "work" key, the result from the encryption is an encrypted "work" key. Similarly, regardless of whether a work key is used to encrypt a secure "scrambling" key, the result from the encryption is an encrypted "scrambling" key. The encryptor 608 simply encrypts a given type of key, but the input and the output of the encryptor 608 remain the same type of key."
>
> • In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that **the features upon which applicant relies (i.e., "The encryptor 608 simply encrypts a given type of key, but the input and the output of the encryptor 608 remain the same type of key") are not recited in the rejected claim(s).** Although the claims are interpreted in light of the specificaion [sic], limitations from the specification are not read into the claims. See In re Van Geuns, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Examiner is interpreting the current language of the claim such that as long as the key that encrypt the secure key is also a secure key, it reads onto the claimed limitation. Since the master key of Akiyama is only provided to the subscriber through smart cards, the master key of Akiyama is in fact a "secure key". Claim language does not require the key that encrypts the secure key to be of same type. Furthermore appellant's own disclosure also allow the secure key to be any of master key, work key and/ or scrambling key (see claim 6 and paragraph 0028, "The secure key may be a master key, a work key and/or a scrambling key."). Therefore, appellant argument that if

> examiner interpret secure key to be work key then the key that encrypts the work key needs to be work key is not found persuasive. Therefore, the combination of Akiyama and Ellison still discloses all the limitations and the rejection should be maintained.

The Appellant respectfully disagrees. Appellant's claim 1 recites "said previously generated unreadable digitally signed and encrypted secure key was generated by encrypting a previously generated digitally signed secure key." In addition, as explained above in section I-A, if an encrypting module encrypts one type of key, then the encrypted output is the same type of key. Therefore, Appellant's claim 1 and the specification support the statement that the input and the output of the encryptor (e.g., 608) remain the same type of key.

The Appellant respectfully submits that independent claims 1, 11, 21 and 32 are allowable.

CONCLUSION

The Appellant submits that the pending claims are allowable in all respects. Reversal of the Examiner's rejections for all the pending claims and issuance of a patent on the Application are therefore requested from the Board.

The Commissioner is hereby authorized to charge additional fee(s) or credit overpayment(s) to the deposit account of McAndrews, Held & Malloy, Ltd., Account No. 13-0017.

Respectfully submitted,

Date: 06-APR-2010

By: /Ognyan I. Beremski/
Ognyan I. Beremski
Reg. No. 51,458
Attorney for Appellant

McANDREWS, HELD & MALLOY, LTD.
500 West Madison Street, 34th Floor
Chicago, Illinois 60661
Telephone: (312) 775-8000
Facsimile: (312) 775-8100

(OIB)